In the Specification:

On page 4, please replace the second paragraph starting on line 5 with the following rewritten paragraph:

a1

Briefly, an information security network provides a plurality of trusted authorities configurable in a rooted hierarchical structure. At least one of the trusted authorities is a superior authority and at least one of the trusted authorities [are] is a subordinate authorit[ies]y. The trust authorities are capable of issuing digitally signed data structures, referred to as certificates. The superior authority is operative to generate policy control message data, such as separate message data or a certificate containing policy information, to dynamically vary policy control data to facilitate trust authority policy delegation among subordinate authorities. The policy control data includes, among other things, inter-trusted authority trust modification data to dynamically vary validation starting authorities among subordinate authorities. The validation starting authorities may use signed data structures (messages, non-messages or any suitable data).

On page 5, please replace the second paragraph starting on line 18 and continuing to page 6, with the following rewritten paragraph:

a2

The superior authority 12 generates policy control message data 20a, 20b and 20c which may be in the form of a signed data structure such as an X.509 certificate or a non-signed data structure if desired. The policy control message data 20a - 20c is used to dynamically vary policy control data among subordinate trust authorities to delegate policy control from the superior authority. As such, the policy control message data 20a - 20c dynamically varies validation starting authorities among subordinate authorities where subordinate trust authorities use the information to change the trust anchor for a given subscriber unit. The dashed lines 22a and 22b represent that a cross certification has been authorized by the data in the policy control

message data 20 - 20c. The lines 24a - 24n represent a trust relationship initially between a subscriber and a starting trust authority. The lines 26a - 26n represent communication links between the respect[ed]ive trust authorities and the X.509 repository to store and retrieve information stored therein, such as certificate revocation list (CRL) information and certificates. In operation, the root trust authority or superior authority 12 effectively generates data that is extracted by subordinate authorities to allow a subordinate authority to execute and define policy control. For example, the subordinate authority may be allowed to cross certify with another specified subordinate authority as dictated by the superior authority 12, thus allowing distributed control of trust anchors so that a subscriber's trust anchor changes from one CA to a different CA under control of a superior authority. In addition, the policy control message data 20a - 20c may indicate that the subordinate authorities can certify other subordinate authorities or only subscribers. Other policy information that may be set forth in the policy control message data 20a - 20c may be, for example, what password rules should be used by the subordinate certification authority. In addition, the subordinate trust authorities create certificates for respective subscribers and also specify, if desired, one or more trust anchors for subscribers. The mechanism to provide the policy control message data 20a - 20c can take many forms, for example, the information may be published in a certificate which may include, for example, digitally signed structures including policy information and rules that should be followed by a subordinate trust authority. The certificates or information may be obtainable through a public directory or by communicating this information directly to the subordinate authority such as store and forward communication or session oriented communications, in a secure manner if desired.

On page 6, please replace the second paragraph, starting on line 30 and continuing to page 7, with the following rewritten paragraph:

FIG. 2 shows by way of example, the superior authority 12 having a policy control message data generator 30 and a trust anchor modification data certificate issuer 32. The policy control message data generator 30 generates policy control message data 34 to control which policy data is to be delegated or communicated to a subordinate authority or a plurality of subordinate authorities The trust anchor modification data certificate issuer 32 creates a trust anchor modification data certificate [20a]21 which includes the signature of the superior authority 12.

On page 9, please replace the second paragraph, starting on line 29 and continuing to page 10, with the following rewritten paragraph:

The trust anchor inter-modification data certificate issuer 32 generates the trust anchor modification data certificate [20a]21 by applying a digital signature to the policy control message data and also includes standard certificate information, such as expiry data and other suitable data. The trust anchor modification data certificate may be generated as a type of X.509 certificate but with the inter-trusted authority trust modification data as a data component. The superior authority 12 then publishes the trust anchor modification data certificate [20a]21 in the repository 18. Alternatively, the superior authority may directly communicate the change in policy information to the requisite subordinate authority if desired.

On page 11, please replace the third paragraph, starting on line 21 and continuing to page 12, with the following rewritten paragraph:

FIG. 3 illustrates by way of example one method of operation of the system. [A]Referring also to FIG. 2 and as shown in block 100, a rooted hierarchical trust authority

structure is provided which includes a root trust authority as well as a plurality of subordinate authorities. The subordinate authorities serve as a trust anchor for various subscribers. The root authority also serves as a trust anchor since the certificate generated by the root authority is trusted by all subscribers in the system. The superior authority as shown by block 102, receives policy modification control data through the graphic user interface that may be provided through the policy control message generator 30. The superior authority 12 generates inter-trusted modification data 34 by incorporating it in a trust anchor modification data certificate 20a. This facilitates the dynamic varying of validation starting authorities for subordinate authorities and/or other subscribers. This is shown in block 104. The inter-trusted modification data may be, for example, the policy control message data. The trust anchor modification certificate issuer 32 incorporates this information into the trust anchor modification data certificate as shown in block 106. As shown in block 108, this information is stored by the superior authority in the repository. On a periodic basis, for example, during each session between a subscriber and a CA, each subordinate authority in the system retrieves the certificates for their respective authority.